REMARKS

Applicants hereby respond to the outstanding final Office Action mailed February 22, 2008. Claims 1, 2, 4-10, 12-17 and 19-33 remain pending hereafter, where claims 1, 9, 17, 22, 23 and 24 are the independent claims.

Claims 1, 2, 9, 10, 17 and 22-33 stand finally rejected under 35 USC §103(a) over US Patent Application Publication No. 2006/0085821 to Simmons, et al. ("**Simmons**") in view of "NPL document :Introduction to SSL" ("**SSL**"). Claims 4-8, 12-16 and 19-21 stand finally rejected under 35 USC §103(a) over **Simmons** and **SSL**, further in view of US Patent Application Publication No. 2003/0177495 to Needham, et al. ("**Needham**").

Response to the Final Rejections Under 35 USC §103(a)

With respect to the independent claims, the Examiner asserts that **Simmons** teaches a video-on-demand (VOD) system, method and computer program product (medium), for demanding a video program via a short message, comprising;

short message generating means for receiving a user demand **(user interface 54; Fig. 2, par. [0040], lines 1-8)**, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field **(paragraphs [0017], [0040], lines 1-15; [0044], lines 22-[0045]; [0052])**;

short message sending means for sending the demand short message generated by the short message generating means **(Network connectivity 12; Fig. 2)**;

demand short message processing means **(transaction server 10, Fig. 1)** at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user, and sending the program identifier of the demanded program by a legal user to video delivering means **(paragraphs [0040], [0044] and [0045])**;

video delivering means **(content providers 6, Fig. 1)** for sending program content corresponding to the program identifier from the program delivering end to the user end indicated by a legal user identifier **(paragraphs ([0040]-[0045])**; and

program playing means at the user end for receiving the video program sent by the video delivering means and playing it back to the user **(42; Fig. 2)**.

The Examiner further states that **Simmons** does not teach implementing security and encryption of content, but that SSL teaches establishing communication between a user and server and authenticating. Once authenticated, encryption is performed using shared keys, and that a format or ciphers to be used are established between client and server **(page 6, 1-3; paragraphs 11, 12).** The Examiner then concludes that it would have been obvious to modify **Simmons'** system to include **SSL** as a security measure, for authenticated and encrypted communication between clients and servers (**SSL**, paragraph 1).

In addition, in the Response to Arguments, the Examiner states that there were no arguments presented as to how the invention as stated in claims 3, 11 and 18 differs from the combined teachings of **Simmons** and **SSL**.

Applicants respectfully assert that **Simmons** combined with **SSL** does realize a video-on-demand system that includes each of the limitations of the independent claims, including the

limitations of cancelled dependent claims 3, 11 and 18, and request reconsideration. For example, applicants' independent claim 9 sets forth:

A Video-on-Demand system for demanding a video program via a short message, comprising:

short message generating means for receiving a user demand, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field, and including an encrypting unit for encrypting the fields in the generated demand short message except the Authentication field;

short message sending means for sending the demand short message generated by the short message generating means;

demand short message processing means at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user, and sending the program identifier of the demanded program by a legal user to video delivering means, and including decrypting means for decrypting the received encrypted short message;

video delivering means for sending program content corresponding to the program identifier from the program delivering end to the user end indicated by a legal user identifier; and

program playing means at the user end for receiving the video program sent by the video delivering means and playing it back to the user. (Emphasis added to reflect the amendments to the claims as set forth in applicants' November 21, 2007, Amendment Under 37 CFR 1.116).

In contrast, **Simmons** at paragraph [0017] states that their player/receiver subsystem enables the home user to connect to a transaction server through a communications network to

access a program guide of media files, and then, via the player/receiver and communications network, requests the transaction server to deliver the requested files. The transaction server authenticates the user request, and verifies the user account, and then transmits a downloaded authorization instruction to the content provider site at which the requested media file is stored. The content provider site then encrypts the requested file, and sends the encrypted file to the user's player/receiver. The encrypted files are decrypted solely by the requesting player/receiver.

Simmons' system (5) is shown in Fig. 1 to include a transaction server (10), network connectivity (12) that connects the transaction server to home user sites (7). The home user site (7) is described in detail with respect to Fig. 2. Home user site (7) comprises a player/receiver subsystem (30) with a user interface 54, system processor 56, system RAM (50), media file decoder (60), media file decryptor (61), TV display interface (40) and audio stereo interface (44). User interface (54) enables the user to request and download selected media files from distributed content provider sites. **Simmons**' paragraph [0040] describes system (5) operation in greater detail, including that player/receiver (30) includes a processor (56) that instructs its network connectivity means (12) to connect to transaction server (10) and transmit a system identifier including a locally generated encryption key and the player/receiver (30) unique electronic serial number and the user's PIN entered via interface (54). The transaction server (10) in turn performs an account authentication operation.

If the user is authenticated, the player/receiver interacts with the transaction server to send requests. The transaction server processes the media requests and generate a transaction ID and instruction data and transmits same along with the user's private encryption key to a content provider site (6). The requested files are encrypted at the content provider site using the private user key and instructions received from the transaction server (10). The encrypted files are sent

to the user at the player/receiver (30), or user interface (54). **Simmons**' Fig. 4 is a detailed view of the transaction server (10), and is described in detail by the text of paragraph [0044]. The transaction server receives the messages sent from a player/receiver (30), which includes the player/receiver serial number, the user's PIN and the local or private encryption key.

SSL, at pages 1 and 2, paragraphs 7 and 8, paragraph 21, numerals 1-10, describe SSL server authentication, SSL client authentication, an encrypted SSL connection and SSL handshake.

The Examiner asserts that **Simmons** teaches short message generating means for receiving a user demand **(user interface 54; Fig. 2, par. [0040], lines 1-8)**, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field **(paragraphs [0017], [0040], lines 1-15; [0044], lines 22-[0045]; [0052])**.

Applicants disagree because neither the **Simmons**' text at paragraphs [0017], [0040], lines 1-15; [0044], lines 22-[0045]; [0052], nor the **SSL** text at pages 1 and 2, paragraphs 7 and 8, paragraph 21, numerals 1-10, whether taken alone or in combination, discloses short message generating means for receiving a user demand, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field, and including an encrypting unit for encrypting the fields in the generated demand short message except the Authentication field. **Simmons**' transaction server (10) is not constructed to decrypt encrypted user messages (demand short messages).

That is, neither **Simmons**' user interface (54) nor player/receiver (30) encrypt demand short messages. **SLL** does not teach or suggest that encryption and decryption is carried out in

the fields in the generated demand short message. For that matter, **SLL**'s disclosed SSL handshake states that a combination of public key and symmetric key encryption is used, but the server authenticates itself to the client, and may request client authentication in a series of signal exchanges (handshaking) between the client and server.

While the Examiner asserts that **Simmons** teaches demand short message processing means **(transaction server 10, Fig. 1)** at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user, and sending the program identifier of the demanded program by a legal user to video delivering means **(paragraphs [0040], [0044] and [0045])**, applicant again respectfully disagree.

Neither the **Simmons**' text at paragraphs [0040], [0044 and [0045], nor the **SSL** text at pages 1 and 2, paragraphs 7 and 8, paragraph 21, numerals 1-10, whether taken alone or in combination, discloses demand short message processing means at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user, and sending the program identifier of the demanded program by a legal user to video delivering means, and including decrypting means for decrypting the received encrypted short message.

Simmons' transaction server (10) is not constructed to decrypt encrypted user messages (demand short messages)--neither Simmons' user interface (54) nor player/receiver (30) encrypt demand short messages. SSL does not remedy the shortcomings of Simmons. While SSL may describe security measures, neither SSL nor Simmons disclose sending the program identifier of the demanded program by a legal user to video delivering means, and including decrypting means for decrypting the received encrypted short message.

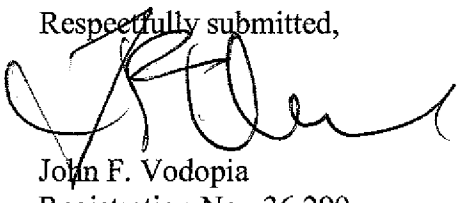
Accordingly, the combination of **Simmons** and **SSL** does not teach or suggest each element of applicants' independent claims. Accordingly, the proposed combination of Simmons and SSL does not render independent claims 1, 9, 17, 22, 23 and 24 unpatentable under 35 USC §103(a). Claims 2, 25 and 26 depend from claim 1 and are patentable therewith; claims 10, 27 depend from claim 9 and patentable therewith. Likewise, claim 28 depends from claim 17 and is patentable therewith, claims 29 and 30 depend from claim 22 and are patentable therewith, and claim 31 depends from claim 23 and patentable therewith. Claims 32 and 33 depend from claim 24 and are patentable therewith. Applicants respectfully request, therefore, that the rejection of pending claims 1, 2, 9, 10, 17 and 22-33 under Section 103(a) over **Simmons** in view of **SSL** be withdrawn.

In response to the rejection of dependent claims 4-8, 12-16 and 19-21 under 35 USC §103(a) over **Simmons** in view of **SSL**, and further in view of **Needham**, applicants respectfully assert that claims 4-8 depend from independent claim 1, claims 12-16 depend from independent claims 9, and claims 19-21 depend from independent claim 17, and are therefore patentable for at least the reasons set forth above for the patentability of independent claims 1, 9 and 17, respectively. Applicants, therefore, request withdrawal of the rejection of claims 4-8, 12-16 and 19-21 under Section 103(a) in view of **Simmons**, **SSL** and further in view of **Needham**.

Conclusion

Accordingly, each of claims 1, 2, 4-10, 12-17 and 19-33 are patentable over **Simmons** in view of **SSL**, whether the combination is taken alone, or in further combination with Needham, and respectfully request withdrawal of the final rejections under Section 103(a), allowance of the claims and passage to issue of the application. If the Examiner believes that a telephone conference with applicants' attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,



John F. Vodopia
Registration No. 36,299
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 913-4666

JFV:vh